Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2773

Vragen van het lid **Oosenbrug** (PvdA) aan de Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *het gebruik van een softwarefout door de Amerikaanse inlichtingendiensten* (ingezonden 27 mei 2015).

Antwoord van Staatssecretaris **Dijkhoff** (Veiligheid en Justitie), mede namens de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie (ontvangen 3 juli 2015). Zie ook Aanhangsel Handelingen, vergaderjaar 2014–2015, nr. 2612

Vraag 1
Heeft u kennisgenomen van het bericht «Het grootste deel van veilige internetverbindingen is kapot»?[1] Bent u op de hoogte van de berichtgeving over de «LogJam bug», die ervoor zorgt dat belangrijke versleutelingsprotocollen te omzeilen zijn?

Antwoord 1
Ja.

Vraag 2 en 3
Heeft u kennisgenomen van het wetenschappelijk artikel, waarin aannemelijk wordt gemaakt dat de National Security Agency (NSA) de kwetsbaarheden in belangrijke versleutelingsprotocollen heeft gebruikt om beveiligde communicatie af te luisteren?[2]
Onderschrijft u de waarneming van de wetenschappers dat gebruik van de nu onthulde kwetsbaarheden in versleutelingsprotocollen een zeer aannemelijke verklaring biedt voor de beveiligde informatie, waarvan afgelopen jaar duidelijk is geworden dat de NSA erover beschikt? Zo nee, waarom niet?

Antwoord 2 en 3
In het wetenschappelijk artikel wordt, naast een uitleg van de Logjam bug, gespeculeerd over de mogelijkheden van de NSA of andere statelijke actoren om als passieve aanvaller (die het internetverkeer tussen een server en een klant uitsluitend registreert en probeert te ontcijferen) het verkeer te kraken.

---

[1] http://politiek.thepostonline.nl/2015/05/25/het-grootste-gedeelte-van-veilige-internetverbindingen-is-kapot/
[2] https://weakdh.org/imperfect-forward-secrecy.pdf

ah-tk-20142015-2773
ISSN 0921 - 7398
’s-Gravenhage 2015

De onderzoekers stellen dat in veelgebruikte communicatieprotocollen (voor beveiligde internetverbindingen, voor geauthentiseerde toegang tot afgeschermde netwerken, of voor mailsystemen) een vercijfermethode gebruikt wordt die gezien de huidige stand van de techniek niet meer veilig geacht wordt, zeker niet als men bescherming tegen grote statelijke actoren nastreeft.
Inlichtingen- en veiligheidsdiensten geven geen inzicht in de wijze waarop zij hun inlichtingen verzamelen in verband met de bescherming van bronnen, modus operandi en actueel kennisniveau. Om die reden is het niet mogelijk een oordeel te geven of de hypothese van de wetenschappers correct is.
In zijn algemeenheid kan ik u wel aangeven dat, dit in lijn met eerdere adviezen van het NCSC, het van belang is om cryptografische producten op de juiste wijze in te stellen en te gebruiken en dat deze instellingen naar de stand der techniek dienen te worden bezien. Het NCSC heeft reeds eerder geadviseerd om van langere sleutellengtes gebruik te maken dan in het artikel worden genoemd.

Vraag 4, 5 en 6
Erkent u het belang van betrouwbare vormen van informatiebeveiliging voor een goed functionerende digitale samenleving? Hoe verhoudt zich dat tot het gebruik of zelfs het actief aanbrengen van kwetsbaarheden door overheden?
Deelt u de mening dat overheden de veiligheid van de digitale samenleving ondermijnen door kwetsbaarheden niet te melden, maar te gebruiken om zich toegang tot informatie en systemen te verschaffen? Zo nee, waarom niet? Zo ja, hoe verhoudt dit gedrag zich tot internationale afspraken om de veiligheid van de digitale samenleving te vergroten?
Maken de Nederlandse inlichtingendiensten en de politie ook gebruik van onbekende kwetsbaarheden? Zo ja, hoe beoordeelt u de ondermijning van de veiligheid die door dit gebruik veroorzaakt wordt?

Antwoord 4, 5 en 6
Zoals in de tweede Nationale Cyber Security Strategie (NCSS-2) is aangegeven is cybersecurity, of informatiebeveiliging als onderdeel daarvan, een randvoorwaarde voor privacy en economische en maatschappelijke groei. De in de NCSS-2 ingezette acties richten zich dan ook op het vinden van een balans tussen veiligheid, vrijheid en economische en maatschappelijke groei.
Zoals eerder in de Eerste Kamer, naar aanleiding van de motie van het lid De Vries (PvdA) (Kamerstuk CVIII, nr. N), aangegeven, hecht het kabinet aan het delen van informatie met belangendragers om de impact van kwetsbaarheden te vermijden.
Ik steun het gebruik van beveiliging voor legale doeleinden. Daar waar de overheid in de persoonlijke levenssfeer van burgers treedt, dient dit altijd van een wettelijke basis en solide waarborgen voorzien te zijn.
Ter versterking van de digitale veiligheid van Nederland en het beperken van de criminaliteit stimuleer ik ook het melden van kwetsbaarheden, onder meer met het beleid voor responsible disclosure. Ook internationaal hecht het kabinet hier sterk waarde aan en zal het belang van responsible disclosure dan ook blijven uitdragen.
Zoals eerder is aangegeven in de beantwoording op de vragen van het lid Gesthuizen (SP) over het gebruik van omstreden spionagesoftware door de politie (kenmerk 566118), brengt het verstrekken van informatie over welke specifieke software de opsporingsdiensten beschikken, testen en gebruiken grote risico's met zich mee voor de inzetbaarheid van die middelen. De verwerving van dergelijke middelen vindt bij de politie onder geheimhouding plaats. Zoals reeds aangegeven, is het gebruikelijk dat inlichtingen- en veiligheidsdiensten geen inzicht geven in de wijze waarop zij inlichtingen verzamelen in verband met de bescherming van bronnen, modus operandi en het actueel kennisniveau. Ik kan hier derhalve geen nadere informatie over verstrekken.
Bij de uitvoering van hun wettelijke taken kunnen de inlichtingen- en veiligheidsdiensten stuiten op onbekende kwetsbaarheden op het internet. Indien zij stuiten op significante kwetsbaarheden die de belangen van gebruikers op het internet kunnen schaden, dan zullen belangendragers geïnformeerd worden.
Indien de politie bij de uitoefening van haar taken op kwetsbaarheden stuit, waarvan bekend is dat het nog niet eerder onderkende kwetsbaarheden

betreft en die de belangen van gebruikers op het internet kunnen schaden, dan zal in samenwerking met het NCSC worden bezien op welke wijze en welke termijn de informatieverstrekking plaatsvindt.
Er kunnen echter wettelijke bepalingen (de wettelijke plicht tot het beschermen van bronnen of actueel kennisniveau) of operationele redenen zijn, die openbaarmaking van kwetsbaarheden (tijdelijk) in de weg staan.
Geconstateerde kwetsbaarheden hoeven overigens niet noodzakelijkerwijs betrekking te hebben op alle gebruikers van het internet, maar kunnen ook specifieke doelgroepen betreffen. Belangendragers zijn dan ook niet per definitie alle gebruikers van internet, dit verschilt per casus. Daarbij wordt het belang van informatieverstrekking afgewogen tegen het belang van geheimhouding en bronbescherming. De diensten werken nauw samen met het Nationaal Cyber Security Centrum (NCSC) en dragen zo vanuit hun expertise bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Vraag 7
Op welke wijze gaat de Nederlandse overheid om met al dan niet bewust aangebrachte kwetsbaarheden in software en hardware? Ondersteunt u de actieve opsporing van dergelijke kwetsbaarheden? Wordt er in aanbestedingen rekening gehouden met de mogelijke aanwezigheid van kwetsbaarheden? Worden kwetsbaarheden, die ontdekt worden, altijd gemeld zodat andere gebruikers zich hiertegen kunnen beveiligen?

Antwoord 7
De Nederlandse overheid is er zich van bewust dat hard- en software kwetsbaarheden kan bevatten. Vanuit het NCSC worden, conform haar reguliere rol, partners en achterban van Rijk en vitale sectoren op dagelijkse basis geadviseerd over kwetsbaarheden in hard- en software en de wijze waarop deze kunnen worden verholpen, bijvoorbeeld door uitvoeren van updates. In Nederland, wordt middels de ontstane praktijk van responsible disclosure, ofwel het op verantwoorde wijze openbaar maken van kwetsbaarheden actief door overheid, bedrijfsleven en beveiligingsonderzoekers en ethische hackers samengewerkt aan het opsporen en verhelpen van kwetsbaarheden.
Bij inkooptrajecten wordt onder meer gewerkt met de beveiligingsrichtlijnen voor webapplicaties van het NCSC. Thans worden deze geactualiseerd, waarbij aandacht zal zijn voor het opnemen van het onderwerp responsible disclosure in deze beveiligingsrichtlijnen. De geactualiseerde versie zal nog dit jaar worden gepubliceerd.
Zoals reeds aangegeven zullen belangendragers worden geïnformeerd over significante kwetsbaarheden die de belangen van gebruikers op het internet kunnen schaden. Er kunnen echter wettelijke bepalingen (de wettelijke plicht tot het beschermen van bronnen of actueel kennisniveau) of operationele redenen zijn, die openbaarmaking van kwetsbaarheden (tijdelijk) in de weg staan.

Vraag 8 en 9
Hoe informeert het Nationaal Cyber Security Centrum (NCSC) bedrijven en burgers bij de ontdekking van ingrijpende kwetsbaarheden als bij deze «LogJam bug»? Welke mogelijkheden zijn er om de risico's van deze kwetsbaarheid te minimaliseren?
Voert het NCSC of een andere partij onderzoek uit naar de mate waarin de Nederlandse digitale infrastructuur, in het bijzonder die van de overheid, getroffen is door deze kwetsbaarheid? Zo nee, wilt u hiertoe opdracht geven?

Antwoord 8 en 9
Het NCSC heeft direct na de publicatie van het wetenschappelijke artikel d.d. 20 mei jl. over kwetsbaarheden in: VPN (Virtual Private Networks, ofwel beveiligde tunnels bv ten behoeve van thuiswerken), TLS (Transport Layer Security, bv voor de beveiliging van web en mailverkeer) en SSH (Secure Shell, bv voor het op afstand beheren van servers) conform haar reguliere rol contact gelegd met haar partners en haar achterban van Rijk en vitale sectoren en deze geïnformeerd over de in het paper genoemde kwetsbaarheid. Dit sluit aan op eerdere adviezen over kwetsbaarheden in deze protocollen. Indien het bij kwetsbaarheden noodzakelijk is om burgers van

handelingsperspectief te voorzien dan wordt gebruik gemaakt van de samen met de Minister van Economische Zaken en ECP[3] ingerichte website www.veiliginternetten.nl.
Uiteraard blijft het NCSC deze problematiek nauwgezet volgen en zal indien noodzakelijk gepaste actie ondernemen. Het is belangrijk om hierbij aan te geven dat de staande beveiligingsadviezen, zoals de ICT-beveiligingsrichtlijnen voor Transport Layer Security, ofwel TLS, hiermee onverminderd van kracht blijven. Door het toepassen van deze richtlijnen, wordt de impact van de kwetsbaarheid geminimaliseerd. Deze richtlijnen zijn voor een ieder te vinden op www.ncsc.nl. In deze richtlijnen is reeds ingegaan op de in het paper genoemde soort kwetsbaarheden en het advies is dan ook om producten consequent in te stellen volgens een hoge standaard van beveiliging.
Specifiek ten aanzien van Open VPN NL, het door de AIVD (NBV) goedgekeurde product voor beveiligd thuiswerken (tot en met het niveau Departementaal Vertrouwelijk), kan aangegeven worden dat het conform het inzetadvies niet vatbaar is voor de genoemde kwetsbaarheid.
Dit in combinatie met het feit dat de ICT-beveiligingsrichtlijnen voor webapplicaties, zoals gebruikt bij de DigiD-assesments, thans worden aangevuld met de ICT-beveiligingsrichtlijnen voor TLS, geeft geen aanleiding om te veronderstellen dat de kwetsbaarheden een majeure impact op de overheid hebben. Een aanvullend onderzoek wordt daarom niet noodzakelijk geacht.

[3] ECP is een neutraal platform van bedrijfsleven, overheid en maatschappelijke organisaties en heeft tot doel het gebruik van ICT in de Nederlandse samenleving te versterken.